1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202.719.7000
FAX 202.719.7049

7925 JONES BRANCH DRIVE
McLEAN, VA 22102
PHONE 703.905.2800
FAX 703.905.2820

www.wileyrein.com

November 21, 2007

Nancy J. Victory
202.719.7344
nvictory@wileyrein.com

VIA ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Ex Parte Presentation*, WT Docket Nos. 96-86, 96-198, 99-87, 01-289, 01-309, 02-55, 06-150, 06-169, 07-166; ET Docket No. 04-295; WC Docket Nos. 04-36, 05-196, 06-63; EB Docket Nos. 04-296, 06-119; CC Docket Nos. 92-105, 94-102; PS Docket Nos. 06-229, 07-114; CG Docket No. 03-123; RM-11376

Dear Ms. Dortch:

Pursuant to Section 1.1206 of the Commission's Rules, I hereby submit *Homeland Security and Communications: A Compendium of Federal Programs* in the above-referenced dockets. Courtesy copies were delivered today to Chairman Kevin J. Martin, Commissioner Michael J. Copps, Commissioner Jonathan S. Adelstein, Commissioner Deborah Taylor Tate, Commissioner Robert M. McDowell, Scott Bergmann, Breck Blalock, Amy Blankenship, Catherine Bohigian, Rudy Brioche, Kirk Burgee, Fred Campbell, Michelle Carey, Rick Chessen, Jeff Cohen, Monica Shah Desai, Scott Deutchman, Ian Dillner, Helen Domenici, Michele Paula Ellison, Samuel Feder, Lisa Fowlkes, David Furth, Angela Giancarlo, John Giusti, Aaron Goldberger, Daniel Gonzalez, Bruce Liang Gottlieb, Rosemary Harold, John Hunter, Ira Keltz, Julius Knapp, Wayne Leighton, Nicole McGinnis, Chris Moore, Kenneth Moran, Barry Ohlson, Erika Olsen, Joseph Palmore, Christina Chou Pauze, Timothy Peterson, Derek Poarch, Roderick Porter, Ron Repasi, James Schlichting, Catherine Seidel, Dana Shaffer, Roy Stewart, and Julie Veach. If you have any questions regarding this presentation, please contact the undersigned.

Respectfully submitted,

/s/ *Nancy J. Victory*

Nancy J. Victory

Attachment

Homeland Security and Communications:

A Compendium of Federal Programs

Prepared by:

Nancy J. Victory
Catherine M. Hilke

November 2007

Introduction

The importance of communications in meeting homeland security needs of the United States is recognized in a large number of wide ranging federal programs and initiatives. This updated survey attempts to capture and categorize legislation pending before Congress, programs administered by the U.S. Department of Homeland Security, the role of the U.S. Department of Justice, activities arising before the Federal Communications Commission, and efforts at other government agencies and departments. The attached matrices reflect a best efforts attempt to provide a simple and timely overview of these complex, interrelated, and dynamic efforts.

About the Authors

Nancy J. Victory
202.719.7344
nvictory@wileyrein.com

Ms. Victory is a partner in the Communications Practice and chair of the International Telecommunications Practice, where she advises a broad cross-section of the industry on the business implications of regulatory policy. Previously she served as Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration under President Bush. Ms. Victory served as the Chair of the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks. She received her J.D., *cum laude* from the Georgetown University Law Center.

Catherine M. Hilke
202.719.7418
chilke@wileyrein.com

Ms. Hilke is an associate in the Communications Practice, where she is engaged in a wide variety of regulatory issues affecting the wireless industry. She received her J.D., *magna cum laude* from the Columbus School of Law, The Catholic University of America.

Table of Contents

FEDERAL COMMUNICATIONS COMMISSION 1

Spectrum 1

Spectrum Efficiency 3

Emergency Alerting 5

911 6

CALEA 8

Katrina 9

Airplane Communications 10

Bureaus/Committees 11

U.S. CONGRESS 13

Spectrum 13

Interoperability 14

Homeland Security Communication Grants 17

9/11 Commission Recommendations 20

Cybersecurity and Critical Infrastructure 22

Emergency Broadcasting 26

Communications Surveillance 27

E-911 and Citizen Emergency Communications 30

U.S. DEPARTMENT OF HOMELAND SECURITY 32

Interoperability 32

Network Security and Reliability 38

Priority Service 46

Emergency Alerting 48

Other 49

U.S. DEPARTMENT OF JUSTICE 50

Interoperability 50

U.S. DEPARTMENT OF COMMERCE 52

Interoperability 52

U.S. DEPARTMENT OF AGRICULTURE 55

Interoperability 55

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES 56

Interoperability 56

Federal Communications Commission

SPECTRUM			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
700 MHz FCC 07-132 WT Docket No. 06-150 CC Docket No. 94-102 WT Docket No. 01-309 WT Docket No. 06-169 PS Docket No. 06-229 WT Docket No. 96-86 WT Docket No. 07-166	The 700 MHz Band is currently used for the broadcast of analog television signals. This spectrum will be returned to the FCC upon completion of the Digital Television Transition, scheduled for February 17, 2009. Under the Digital Television and Public Safety Act of 2005, Congress allocated 24 MHz of the 700 MHz Band for public safety communications (the rest will be auctioned for commercial uses). Half of this spectrum has been set aside for narrowband voice communications services that must be provided under rigid technical standards designed to promote interoperability. The other half will be designated for interoperable broadband communications. The FCC adopted the following requirements for the 700 MHz spectrum. *Public Safety Spectrum*. The Commission will award a nationwide license for the 12 MHz of spectrum designated for broadband communications to a single Public Safety Broadband Licensee. The Public Safety Broadband Licensee will lease access to the spectrum and the deployed network to individual public safety entities. A state or local public safety entity may either (a) build its own broadband network that meets the requirements and specifications of the shared network with pre-approval from the Public Safety Broadband Licensee; or (b) seek a waiver to operate a wideband network that is not inconsistent with an area's broadband deployment plan. *Commercial Spectrum*. The Commission also established service rules for the commercial portions of the 700 MHz Band. Among other things, the FCC concluded that the winner of the 10 MHz "D Block" license will be required to negotiate a network sharing agreement with the Public Safety Broadband Licensee under which the D Block	This decision makes more dedicated spectrum available for public safety communications. The selection of a single licensee will ensure the interoperability of broadband public safety communications. For the first time, it also requires a shared commercial/public safety infrastructure to facilitate build-out of advanced communications technologies for public safety. Additional commercial 700 MHz services also may be a useful tool for public safety.	Order released August 10, 2007. Auction for commercial 700 MHz band, including the "D Block" scheduled to begin January 24, 2008. On November 19, 2007, the Commission released an Order selecting the Public Safety Spectrum Trust Corporation as the single nationwide licensee for the public safety 700 MHz broadband spectrum allocation.

SPECTRUM			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
700 MHz (cont.) WT Docket No. 06-150	licensee will build a network that encompasses both the D Block and the Public Safety Broadband Licensee spectrum. Under this agreement, public safety entities would be allowed to access the D Block commercial spectrum during emergencies.		
Advanced Wireless Services Report No. AUC-06-66-F	In 2006, 104 entities won 1087 licenses to provide advanced wireless services (AWS), including third generation (3G) mobile broadband, in the 1.7 and 2.1 GHz bands. These systems are intended to provide access to a wide range of telecommunications services and other services that are specific to mobile users. The 1.7 GHz band is currently licensed to a variety of federal government entities. The 2.1 GHz band is currently licensed to private and commercial fixed microwave systems. Incumbent licensees in both bands must be relocated by AWS licensees prior to service initiation.	NTIA worked with the Department of Defense and other federal agencies to develop a set of proposals to clear the 1.7/2.1 GHz bands for AWS. Commercial AWS services may be a useful tool for first responders.	AWS licensees are currently in negotiations with federal government incumbents regarding relocation.

SPECTRUM EFFICIENCY			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
800 MHz Rebanding FCC 04-168 FCC 04-294 DA 07-27 DA 07-1648 FCC 07-92 FCC 07-102 WT Docket No. 02-55	Public safety and Commercial Mobile Radio Service (CMRS) providers operate in the 800 MHz band on adjacent frequencies. Due to technical incompatibilities, interference to public safety operations occurred. The FCC required Sprint Nextel to surrender some of its 800 MHz spectrum and fund the relocation of public safety and other incumbents to new frequency assignments in the 800 MHz band. In exchange, the FCC issued Sprint Nextel a license for 10 MHz of spectrum in the 1.9 GHz PCS band. The rebanding process is being implemented by an independent Transition Administrator (TA) comprised of BearingPoint, Squire Sanders Dempsey LLP and Baseline Telecom, Inc. Rebanding began on June 27, 2005 and must be completed by June 26, 2008. On May 30, 2007, the FCC released a Second MO&O addressing petitions for reconsideration in the 800 MHz proceeding. Among other things, the FCC clarified various aspects of relocation to the ESMR band and defined limits on Sprint's operations near the NPSPAC prior to the conclusion of the rebanding.	Reconfiguration of the 800 MHz band is designed to decrease interference between public safety radio systems and commercial systems.	The Wireless Bureau is resolving disputes on a rolling basis. On May 18, 2007, the FCC released a MO&O clarifying the standard for determining the acceptability of costs that Sprint Nextel is required to pay in connection with the 800 MHz rebanding process. On September 12, 2007, the FCC released a MO&O finding that Sprint had not met its 18-month benchmark for clearing Channel 1-120 incumbents from the 800 MHz Band. The Commission did not impose a fine or forfeiture on Sprint and instead established additional benchmarks to ensure timely clearing of the Channel 1-120 band by all incumbent licensees, including Sprint. Specifically, the MO&O required that Sprint (1) clear all remaining incumbents on channels 1-120 by December 26, 2007; (2) clear its own use of these channels within 90 days of any public safety request (within 60 days for any request made after January 1, 2008); (3) submit monthly progress reports; and (4) clear all non-cellular channels in the 800 MHz band by June 2008. On October 12, 2007, Sprint filed a suit challenging the FCC's MO&O in the U.S. Court of Appeals for the D.C. Circuit. The deadline for initial filings is November 14.

SPECTRUM EFFICIENCY			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
800 MHz Rebanding (cont.) WT Docket No. 02-55			On September 12, 2007, the FCC also issued a public notice outlining supplemental procedures and providing guidance for completion of 800 MHz rebanding by National Public Safety Planning Advisory Committee (NPSPAC) licensees.
Transition to 6.25 kHz Narrowband Technology by PLMR Systems FCC 07-39 FCC 04-292 WT Docket No. 99-87 RM-9332	The FCC has established the following transition for requiring the use of more efficient technologies in certain land mobile frequency bands at 150-174 MHz and 421-512 MHz. The following deadlines are now in force: – On January 1, 2013, all private land mobile licensees (Business, Industrial and Public Safety) must operate with technology designed to operate within a 12.5 kHz channel. Broader bandwidth technologies are permitted provided that they offer equivalent efficiency. – Applications for new or modified operations on 25 kHz channels will be accepted until January 1, 2011. After that date, applications specifying bandwidths greater than 12.5 kHz will be accepted only for equivalent efficiency designs. – Manufacturers can continue to build and import equipment operating on channel bandwidths up to 25 kHz until January 1, 2011. After that date, the manufacture and importation of such equipment operating on a channel bandwidth greater than 12.5 kHz will be limited to equivalent efficiency designs. – Beginning January 1, 2011, equipment certification applications must specify 6.25 kHz capabilities.	The "refarming" proceedings modified technical standards and operating conditions for public safety operations in the Public Safety Pool, allowing for the development of more advanced and efficient public safety services.	In March 2007, the FCC declined to establish a fixed date for private land mobile radio systems in the 150-174 MHz and 421-512 MHz bands to transition to 6.25 kHz narrowband technology, but strongly urged licensees to consider migrating directly to 6.25 kHz rather than first adopting 12.5 kHz technology and later migrating to 6.25 kHz technology. The Commission also required that certain equipment certification applications specify 6.25 kHz capabilities by January 1, 2011.

EMERGENCY ALERTING			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Next Generation Emergency Alert System Rulemaking FCC 07-109 EB Docket No. 04-296	The Next Generation Emergency Alert System (Next Generation EAS) enables the President of the United States, state officials, and the National Weather Service to address the nation during an emergency by providing communications capability from broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, and direct broadcast satellite services. In its July 12, 2007 Second R&O and FNPRM, the FCC required Next Generation EAS participants to accept text, audio, and video messages using the Common Alerting Protocol (CAP). It also sought comment on how to deliver warnings to persons with disabilities and non-English speakers, and how to ensure that the Next Generation EAS system will operate as intended.	The Next Generation EAS gives the government the ability to alert the public through a variety of media in case of an emergency or disaster.	Comments on the FNPRM are due December 3, 2007; Reply Comments are due December 17, 2007.
Commercial Mobile Service Alert Advisory Committee DA 07-2935	Consistent with section 603 of the Warning, Alert and Response Network Act (WARN Act), the FCC established the Commercial Mobile Service Alert Advisory Committee (CMSAAC). The CMSAAC's mission is to develop recommendations on technical standards and protocols to facilitate the ability of commercial mobile service providers to voluntarily transmit emergency alerts to their subscribers.	The recommendations of the committee are designed to allow important emergency messages to be widely circulated to wireless handsets.	The CMSAAC held its final meeting on October 3, 2007 where it considered and voted on its recommendations. The CMSAAC's recommendations were submitted to the Commission on October 12, 2007, but have not yet been made public. Under the WARN Act § 602, the FCC is required to complete a proceeding to adopt relevant technical standards within 180 days of CMSAAC's submittal of recommendations.

911			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Wireless E911 and Voice over Internet Protocol E911 Requirements FCC 07-108 PS Docket No. 07-114 WC Docket No. 05-196	Enhanced 911 (E911) enables emergency service providers to accurately pinpoint the location of a 911 caller. The FCC currently requires Commercial Mobile Radio Service providers to provide Public Safety Answering Points with automatic number information and automatic location information. The FCC is also considering whether providers of nomadic interconnected Voice over Internet Protocol (VoIP) should be required to provide E911 automatic location information. On June 1, 2007, the FCC adopted a NPRM regarding location accuracy and reliability requirements for wireless E911 and VoIP 911 services. Specifically, the FCC sought comment on its tentative conclusion that licensees should be required to meet E911 Phase II location requirements at a PSAP level. The FCC also sought comment on, among other things, its tentative conclusion to establish a single location accuracy requirement irrespective of technology; whether a more stringent accuracy requirement should be adopted; the methodology for accuracy compliance testing; and the establishment of a mandatory schedule for accuracy testing.	The wireless E911 rules were designed to improve the effectiveness and reliability of wireless 911 service by providing 911 dispatchers with additional information on wireless 911 calls.	On August 30, 2007, the FCC released 3 Notices of Apparent Liability for Forfeiture against Sprint, Alltel, and U.S. Cellular for failure to meet the December 31, 2005 deadline for achieving 95 percent penetration of location-capable handsets. On September 11, 2007, the FCC adopted a Report and Order on the geographic scope of the current wireless location accuracy requirements. Specifically, the FCC clarified that wireless carriers must meet E911 Phase II location requirements at a PSAP level by September 11, 2012. The FCC also adopted interim benchmarks under which carriers must fulfill its location accuracy requirements within each Economic Area by September 11, 2008 and within each Metropolitan Statistical Area and Rural Service Area level by September 11, 2010. Carriers also must demonstrate significant progress toward compliance at the PSAP-level, including achieving this requirement within at least 75 percent of the PSAPs the carrier serves, by September 11, 2010. Comments on whether the FCC's current E911 location requirements should be revised were due on August 20, 2007, and reply comments on September 18, 2007.

911			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
VoIP Disability Access Requirements FCC 07-110 WC Docket No. 04-36 WT Docket No. 96-198 CG Docket No. 03-123 CC Docket No. 92-105	Under section 255, manufacturers of telecommunications equipment and providers of telecommunications service must ensure that their equipment or service is accessible to and usable by individuals with disabilities to the extent readily achievable. Section 225 requires, among other things, VoIP providers to contribute to the Telecommunications Relay Services Fund and to offer 711 abbreviated dialing for access to relay services.	The Section 255 requirements will ensure that individuals with disabilities will be able to take advantage of VoIP 911 services.	On June 15, 2007, the FCC adopted a Report and Order extending the disability access requirements of sections 225 and 255 of the Communications Act to interconnected Voice over Internet Protocol (VoIP) services and to manufacturers of specially designed equipment used to provide those services.

CALEA			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
CALEA Wiretapping FCC 05-153 FCC 06-56 ET Docket No. 04-295 Report No. 2816 DA 07-2522 RM-11376	Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. This law requires telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. CALEA applies to all telecommunications carriers as defined by Section 102(8) of CALEA, including entities engaged in the transmission or switching of wire or electronic communications as common carrier for hire. A telecommunications carrier must ensure that its equipment, facilities, and services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of meeting the assistance capability requirements.	CALEA preserves the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology.	Facilities-based broadband Internet services and interconnected VoIP services must have complied with CALEA requirements by May 14, 2007. On May 15, 2007, the DOJ, FBI, and DEA filed a "Petition for Expedited Rulemaking" requesting the FCC to initiate a proceeding to find that the J-STD-025-B is deficient pursuant to Section 107(b) of CALEA and mandate the inclusion of four additional or modified intercept capabilities in the J-STD-025-B with respect to CDMA2000 packet data wireless services. These capabilities are: packet activity reporting; provision of more granular mobile handset location information at the beginning and end of a communication; service quality, including security, performance and reliability requirements; and timing information (time stamping). Comments on the Petition for Expedited Rulemaking were due July 25, 2007 and Reply Comments on September 25, 2007.

KATRINA			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks FCC 07-107 EB Docket No. 06-119 WC Docket No. 06-63	The Katrina Panel was established to review the impact of Hurricane Katrina on communications infrastructure and to recommend ways to improve network reliability and communication among emergency response services. On June 8, 2007, the FCC released an order (revised on reconsideration on October 4, 2007) in response to the Panel's recommendations. The FCC (1) Required communications providers to (a) have emergency/back-up power for all assets regardless of the type of commercial power, including those inside cell sites, unless precluded by law, public safety, or prior contract and (b) conduct analyses and submit reports on their back-up power compliance and the redundancy and resiliency of their 911 and E911 networks; (2) Instructed the Public Safety and Homeland Security Bureau (PSHSB), among other things, to develop and implement an awareness program to educate public safety agencies about alternative communications technologies, work with other federal agencies on developing credentialing standards for communications service providers and facilitating first responder interoperability, take steps to revitalize and publicize the current Emergency Alert system, and reach out to the emergency medical community to facilitate the resiliency and effectiveness of their emergency communications systems; and (3) Extended regulatory relief from section 272 of the Communications Act of 1934.	The Katrina Panel's recommendations and the directives in the ensuing order are designed to improve communication among emergency response services.	The PSHSB must report on its efforts 3 months and 9 months after the release of the June 8, 2007 order. Consistent with the FCC's June Order, the PSHSB launched a newly designed and automated Disaster Information Reporting System (DIRS) on September 11, 2007. DIRS is a voluntary, web-based system that communications companies, including wireless, wireline, broadcast, and cable providers, can use to report communications infrastructure status and situational awareness information during times of crisis. The back-up power requirements become effective on the date that OMB approval of the information collection requirements is published in the Federal Register. Reports on compliance with the back-up power requirements are due within six months of the effective date. LECs and CMRS providers identifying assets in their reports that are designed with less than the required emergency backup power capacity (and not otherwise precluded from compliance) must comply with the backup power requirement or file a certified emergency backup power compliance plan within 12 months from the effective date.

AIRPLANE COMMUNICATIONS			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Aeronautical Mobile Satellite Service FCC 06-148 WT Docket No. 01-289	Aeronautical Mobile Satellite Service (AMSS) is a mobile service between aeronautical stations and aircraft stations, or between aircraft stations. The service provides two-way communications, including broadband, onboard aircraft. The services, including certain frequency bands and technical standards used for this service, are coordinated internationally through the International Civil Aviation Organization to ensure the worldwide interoperability. In October 2006, the Commission adopted a Second R&O and FNPRM addressing and seeking comment on a number of issues pertaining to the Aviation Radio Service.	Many of the communications within this service are used for air traffic services and aeronautical operational control safety communications. Broadband capability for crews is intended to enhance aircraft operations through real time equipment and supply information, weather updates, and security monitoring.	This proceeding remains pending.

BUREAUS/COMMITTEES			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Public Safety and Homeland Security Bureau FCC 06-35	On September 25, 2006, the FCC established the Public Safety and Homeland Security Bureau (PSHSB). It is designed to address public safety functions that were previously dispersed among different bureaus. Those functions include public safety, homeland security, national security, disaster management, and emergency management and preparedness.	The PSHSB is the main bureau for FCC issues that deal with homeland security and public safety communications.	On February 23, 2007, Chairman Kevin J. Martin announced his intention to appoint Derek Poarch as Chief of the PSHSB. Prior to joining the FCC, Chief Poarch was Director of Public Safety and Chief of Police at the University of North Carolina at Chapel Hill. On September 25, 2007, PSHSB hosted a Summit on Communications Network Surge Management in Emergencies. The Summit examined how communications networks are managed during mass emergency situations. On November 1, 2007, PSHSB, in conjunction with the U.S. Department of Health and Human Services hosted a Health Care Summit on Emergency Communications, Response and Recovery. The Summit focused on hospital emergency communications plans and preparedness efforts and will examine the benefits of utilizing broadband networks and other communications infrastructure.
Intergovernmental Advisory Committee DA 07-2427	The Intergovernmental Advisory Committee (IAC) "advises the Commission on a range of telecommunications issues for which their governments explicitly or inherently share responsibility or administration with the Commission."	The IAC addresses homeland security and public safety issues.	The Commission reauthorized the IAC in February 2006 and rechartered the IAC in June 2007. The Commission's authorization lasts for two years. There is an option for reauthorization every two years.

BUREAUS/COMMITTEES			
Initiative/Proceeding	**Description**	**Relevance to Homeland Security**	**Status/Notes**
Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities	On September 7, 2007, the FCC and NTIA announced the establishment of a Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities. The Committee will assess the following: (1) Specific communications capabilities and needs of emergency medical and public health care facilities, including the improvement of basic voice, data, and broadband capabilities; (2) options to accommodate growth of basic and emerging communications services used by emergency medical and public health care facilities; and (3) options to improve integration of communications systems used by emergency medical and public health care facilities with existing or future emergency communications networks.	The Committee will address the communications needs of emergency medical and public health care facilities.	The Committee must report its findings to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce, no later than February 4, 2008. FCC Chairman Kevin Martin and NTIA Assistant Secretary John Kneuer announced the appointment of the members of the Committee on October 18, 2007. The Committee held its first meeting on October 29, 2007.

U.S. Congress

SPECTRUM			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The SAVE LIVES Act, S. 744	Creates the Public Safety Interoperable Communications Working Group to develop specifications for a national public safety broadband network on an additional 30 MHz of 700 MHz spectrum from the DTV transition. Creates a Public Safety Broadband Trust Corporation if no bidder obtains the license. Requires the FCC to complete its ongoing rulemaking regarding a nationwide public safety 700 MHz network (PS Docket No. 06-229; WT Docket No. 96-86) and issue rules to allow certain channels to carry data communications.	Develops a nationwide, interoperable public safety wireless broadband network on 700 MHz.	Sen. John McCain (R-AZ) introduced S. 744 on March 1, 2007, and it was referred to the Committee on Commerce, Science, and Transportation. The FCC recently issued an order adopting rules to govern the creation of a national public safety broadband network.
The Re-Channelization of Public Safety Spectrum Act, H.R. 1788	Re-channelizes upper 700 MHz public safety spectrum to accommodate commercially available broadband data applications.	Seeks interoperability between first responder systems and commercial wireless data devices.	Rep. Mike Ferguson (R-NJ) introduced H.R. 1788 on March 29, 2007, and it was referred to the House Committee on Energy and Commerce.

INTEROPERABILITY			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Improving Communications Interoperability Grant Program Act, H.R. 338, H.R. 863	Establishes the Improve Communications for Emergency Response Grant Program in order to improve and achieve statewide, regional, national, and international interoperability. Authorizes funding only after substantial progress has been made towards voluntary, consensus-based interoperable communications standards.	Authorizes interoperability grants for: planning, design and engineering, procurement and installation, exercises, modeling and simulation, and technical assistance.	Rep. John Dingell (D-MI) introduced H.R. 338 on January 9, 2007, and it was referred to the Committee on Energy and Commerce, where Rep. Dingell is Chairman. Rep. Bennie Thompson (D-MS) introduced H.R. 863 on February 6, 2007, and it was referred to the Committee on Homeland Security, where Rep. Thompson is Chairman. The bill was also referred to the Committee on Energy and Commerce on that same day.
The Interoperable Emergency Communications Act, S. 385	Makes changes to the $1 billion interoperable communications grant program funded by the DTV transition's upcoming 700 MHz spectrum auction. Prioritizes grants based on risk and requires recipients to provide information on interoperability. Specifies that grants may be awarded only to systems compatible with SAFECOM guidelines (*see* P.L. 108-408 § 7303). Earmarks $100 million for strategic, pre-positioned reserves of interoperable communications. Requires reports on back-up communications systems for first responders and the status of cross-border international interoperability negotiations and issues.	Makes modifications to existing public safety communications grant programs to improve effectiveness.	Sen. Daniel Inouye (D-HI) introduced S. 385 on January 24, 2007, and it was referred to the Committee on Commerce, Science, and Transportation, where he is Chairman. The legislation was then reported out of the Committee and placed on the Senate Legislative Calendar on March 5, 2007. The bill refers to the grant program established by Sec. 4 of the Call Home Act of 2006 (P.L. 109-459), which requires the award of $1 billion in public safety grants by September 30, 2007.

INTEROPERABILITY			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The DHS Appropriations Act for FY2008, H.R. 2638, S. 1644	H.R. 2638 provides $178 million ($238 million in S. 1644) to the Department of Homeland Security for information technology. Both bills include $33 million for a secure DHS network with state and local agencies. The House bill specifically provides $50 million for first responder interoperability grants and $10 million for interoperable communications technical assistance. The House report (110-181) encourages DHS to evaluate IP-based interoperability and consider amending SAFECOMM accordingly. S. 1644, as introduced, included no specific interoperability grants and provides $24 million for interoperability technical assistance. Sen. Lieberman (ID-CT) included an amendment during Senate consideration of H.R. 2638 to provide $100 million for first responder interoperability grants.	Provides additional funding and direction to improve the interoperability of federal, state and local public safety entities.	Rep. David Price (D-NC), the Chairman of the DHS Appropriations Subcommittee of the House Appropriations Committee, introduced H.R. 2683 on June 8, 2007. The House approved H.R. 2683 by a vote of 268 to 150 on June 15, 2007. Sen. Robert Bryd (D-WV), the Chairman of the Senate Appropriations Committee introduced S. 1644 on June 18, 2007. The Senate replaced the text of H.R. 2683 with S. 1644, and approved H.R. 2683 by a vote of 89 to 4 on July 26, 2007. A House-Senate conference will meet to resolve differences between the bills.
The Public Safety Interoperability Implementation Act, H.R. 3116	Establishes a trust fund for public safety communications and interoperability grants. Earmarks unused funds from the DTV 700 MHz spectrum auction and 50% of future auction proceeds for the fund.	Allocates grants for public safety interoperability equipment, planning, training, and research.	Rep. Bart Stupak (D-MI) introduced H.R. 3116 on July 19, 2007, and it was referred to the House Committee on Energy and Commerce.
The 9/11 Can You Hear Me Now Act, H.R. 3199	Directs DHS to develop and provide improved communications equipment, including radios, for the New York City Fire Department.	Provides for improved communications equipment for first responders.	Congresswoman Maloney (D-NY) introduced H.R. 3199 on July 26, 2007, and the legislation was then referred to the House Committee on Energy and Commerce.

INTEROPERABILITY			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Coast Guard Authorization Act for FY 2008, S. 1892.	Directs DHS to assist ports and port facilities in implementing port security anti-terrorism measures. Specifically, DHS is directed to pre-position interoperable communications equipment at interagency operation centers.	Improves communications between port security agencies.	Senator Cantwell (D-WA) introduced S. 1892 on July 26, 2007, and the legislation was referred to the Senate Committee on Commerce, Science, and Transportation.
The Commerce, State, Justice, Science and Related Agencies Appropriations Act of 2008, H.R. 3093, S. 1745	Appropriates funding for the FY 2008 operations of the Departments of Commerce, State, and Justice and other agencies, including $18 million for salaries and expenses at NTIA, a $500,000 increase from FY 2007.	The House Appropriations Committee report instructs NTIA to review public broadcasters data-casting capabilities in light of NTIA's interoperability efforts and report on their potential for state and regional emergency preparedness.	Rep. Alan Mollohan (D-WV) introduced H.R. 3093 on July 19, 2007 and the House approved it on July 26. Sen. Barbara Mikulski (D-MD) reported S. 1745 out of the Senate Appropriations Committee on June 29, 2007. The Senate amended and approved H.R. 3093 on October 19 and a House-Senate conference will meet to resolve differences.

HOMELAND SECURITY COMMUNICATION GRANTS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Urban Area Security Initiative Grant Enhancement and Authorization Act of 2007, H.R. 1020	Requires Urban Area Security Initiative grants to be based solely on risk of a terrorist attack on high-threat, high-density urban areas and not on need-based factors. Allows use of grants for first responder communications.	Makes first responder communications eligible for grants.	Rep. Vito Fossella (R-NY) introduced the bill on February 13, 2007, and it was referred to the House Committee on Homeland Security.
The Homeland Security Trust Fund Act of 2007, S. 345	Creates the Homeland Security and Neighborhood Safety Trust Fund with $53 billion from 2007 to 2011 by reducing 2001 income tax reductions for taxpayers with taxable income over $1 million. Prohibits extensions for the DTV transition that delay the reassignment of spectrum to public safety. Allocates $2 billion per year for the Community Oriented Policing Services (COPS) Program and creates a board to assist with the balance of the funding. Earmarks $1 billion/year of COPS funding for interoperability and it eligible for the balance.	Proposes measures to ensure availability of spectrum for public safety and provides interoperability funding.	Sen. Joe Biden (D-DE) introduced S. 345 on January 22, 2007, and it was referred to the Committee on Homeland Security and Government Affairs.
The Risk-Based Homeland Security Grants Act of 2007, S. 608	Requires homeland security grants to be allocated based on an assessment of threats and vulnerabilities. Requires states to submit 3-year state homeland security plans for approval. Gives prioritization to grants to protect critical infrastructure, and makes protecting critical infrastructure a factor for determining the essential homeland security capabilities of state and local agencies. Requires DHS to support national voluntary consensus standards for first responder equipment, including interoperable communications equipment.	Makes interoperable communications eligible for grants. Includes communications networks as critical infrastructure and cyber threats as a factor for threat assessments.	Sen. Diane Feinstein (D-CA) introduced S. 608 on February 15, 2007, and it was referred to the Committee on Homeland Security and Government Affairs.

HOMELAND SECURITY COMMUNICATION GRANTS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Firefighters Special Operation Task Force Act, H.R. 1351	Authorizes grants to firefighting task forces operating under a cooperative incident report agreement. Allows grants for improving communications and interoperability with local police or hospitals, or any other appropriate entity.	Provides funding for firefighter communications.	Rep. Nita Lowey (D-NY) introduced the bill on March 6, 2007, and it was referred to the House Committee on Science and Technology.
The COPS Improvements Act of 2007, H.R. 1700, S. 368	Revises the grant purposes under the community oriented policing (COPS) program to include the hiring or training of law enforcement officers for intelligence, anti-terror, and homeland security duties along with increased school security and anti-gang activity purposes. Includes interoperable communications as an eligible purpose for technology grants under the Act.	Provides funding for first responder communications.	Rep. Anthony Weiner (D-NY) introduced H.R. 1700 on March 26, 2007. The House approved it on May 15 by a vote of 381 to 34. The Senate received H.R. 1700 on May 16 and referred it to the Committee on the Judiciary on August 3, 2007. Sen. Joe Biden introduced S. 368 on January 23, 2007 and was referred to the Committee on the Judiciary. The Committee reported the bill without amendment to the full Senate on May 24, 2007.
The Domestic Preparedness Act of 2007, H.R. 1715	Authorizes grants to improve homeland security preparedness of municipal and county governments. Eligible purposes include interoperability between members of a consortium of municipal or county governments. Allows Interoperability grants to provide up to 90% of project funding. Requires grants to be made pursuant to terrorism vulnerability assessments conducted by units of local government and to be used for new programs, not to sustain or supplement existing programs.	Provides funding that can be used to facilitate the interoperability of local governments.	Rep. Carolyn McCarthy (D-NY) introduced the bill on March 27, 2007, and it was referred to the House Committee on Homeland Security.

HOMELAND SECURITY COMMUNICATION GRANTS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
School Safety and Law Enforcement Improvement Act of 2007, S. 2084	S. 2084 is a broad piece of law enforcement legislation that covers school safety, the national background check system, and law enforcement officer benefits. The bill creates a grant program for campus law enforcement and security at colleges and universities.	Includes emergency systems for to contact students using state-of-the-art communications as a use of grant funds.	Chairman Leahy introduced S. 2084 and the Senate Judiciary Committee approved the bill on September 21, 2007.

9/11 COMMISSION RECOMMENDATIONS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Implementing the 9/11 Commission Recommendations Act of 2007, H.R. 1 The Improving America's Security Act of 2007, S. 4 (formerly titled the Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007)	H.R. 1 is a broad pieces of legislation intended to implement recommendations of the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission. This summary covers the conference report (110-259) of H.R. 1 which represents the final version merging the two House and Senate bills. Among other items, H.R. 1 authorizes $950 million/year for state homeland security grants and up to $1.3 billion/year for urban high risk grants by 2012. Eligible uses include computer hardware and software, interoperability, protecting critical infrastructure, and 911 public safety answering points. The legislation also creates a National Asset Database to identify and prioritize critical infrastructure; authorizes private sector security guidance and best practices; creates a voluntary private sector preparedness certification program; requires annual reports on critical infrastructure vulnerabilities. Both bills also address interoperability in detail. H.R. 1 authorizes $400 million/year for interoperability grants to states with approved interoperability plans. It prohibits use of grant funds for equipment that does not meet voluntary consensus standards and clarifies the funding may be used for IP-based interoperability solutions. The legislation also requires a status report on interoperability in the Canadian and Mexican border areas.	Legislation provides additional funding for public safety communications systems, critical infrastructure protection and E911 systems.	Rep. Bennie Thompson (D-MS), Chairman of the House Committee on Homeland Security, introduced H.R. 1 on January 5, 2007. The House approved H.R. 1 on January 9, 2007 by a vote of 299 to 128. Sen. Harry Reid (D-NV), Senate Majority Leader, introduced S. 4 on January 4, 2007. The Senate approved S. 4, as amended, by a vote of 60 to 38 on March 13, 2007. The Senate incorporated S. 4 as passed by the Senate into H.R. 1 and unanimously approved H.R. 1 on July 9, 2007, sending H.R. 1 to a House-Senate conference. On July 25, the conference committee approved the conference report for H.R. 1, which was then approved by the Senate on July 26 by a vote of 85 to 8 and by the House on July 27 by a vote of 371 to 40. The President signed this bill on August 3, making it Public Law No. 110-053.

9/11 COMMISSION RECOMMENDATIONS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Ensuring Implementation of the 9/11 Commission Report Act, S. 328	Like H.R. 1 and S. 4, this legislation intends to implement outstanding recommendations of the 9/11 Commission. S. 328 covers: (1) critical infrastructure and private sector preparedness, (2) grants for first responders, (3) transportation and border security, and (4) intelligence and civil liberties.	Prohibits extensions for the DTV transition that delay the reassignment of spectrum to public safety. Includes communications infrastructure as a risk factor to prioritize grants.	Sen. Bob Menendez (D-NJ) introduced S. 328 on January 17, 2007, and it was referred to the Committee on Foreign Relations.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Cybersecurity Education Enhancement Act of 2007, H.R. 263	Provides grants for institutions of higher education for cybersecurity programs. Creates an e-security fellowship program to bring state, local, and private sector officials to participate in DHS's National Cybersecurity Division.	Authorizes grants for cybersecurity training.	Rep. Sheila Jackson-Lee (D-TX) introduced the bill on January 5, 2007, and it was referred to three House Committees: (1) Homeland Security, (2) Science and Technology, and (3) Education and Labor.
The Foreign Investment and National Security Act of 2007, H.R. 556, S. 1610	Makes significant changes to the Committee on Foreign Investment in the United States (CFIUS) process. CFIUS reviews mergers, acquisitions, or takeovers which could result in foreign control of U.S. companies that have security-related impacts on U.S. critical infrastructure. The bill requires CFIUS investigations of foreign government-controlled transactions.	CFIUS may review transactions that involve foreign ownership of critical U.S. communications infrastructure.	Rep. Carolyn Maloney (D-NY) introduced H.R. 556 on January 18, 2007. Chairman Chris Dodd (D-CT) authored S. 1610, and the Senate Banking Committee approved the bill on June 13, 2007. The House approved H.R. 556 on February 28, 2007 by a vote of 423 to 0 and the Senate approved S. 1610 as an amendment to H.R. 556 unanimously. The House then approved the Senate-amended version of H.R. 556 370 to 45. The President signed the bill into law on July 26, 2007, making it Public Law No. 110-49.
Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836	Expands and increases penalties for federal cybersecurity and computer hacking violations. Expands racketeering to include computer fraud, and redefines extortion to include threats to access a computer without authorization.	Provides additional funds for prosecuting criminal activity involving computers.	Rep. Lamar Smith (R-TX) introduced H.R. 836 on February 6, 2007, and it was referred to the Committee on the Judiciary (Rep. Smith is the ranking minority member of the House Committee on the Judiciary).

CYBERSECURITY AND CRITICAL INFRASTRUCTURE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Rail and Public Transportation Security Act of 2007, H.R. 1401, H.R. 1269 The Rail Transit Security and Safety Act of 2007, H.R. 534 The Surface Transportation and Rail Security Act of 2007, S. 184 The Rail Security Act of 2007, S. 83 The Public Transportation Terrorism Prevention Act of 2007, S. 763 The Passenger Rail Investment and Improvement Act of 2007, S. 294.	H.R. 1401 and H.R. 1269 create comprehensive rail and transit security programs including vulnerability assessments and grant programs for freight rail, rail transit, over-the-road bus transit, and tunnel systems. S. 294, S. 184, and S. 83 also require rail vulnerability assessments and the development of prioritized recommendations to improve rail security. S. 184 additionally includes a title on inter-city bus transit and the transportation of hazardous materials, including pipelines. Both S. 184 and S. 83 authorize grants to improve rail security. H.R. 534 and S. 763 require federal security assessments for all high-risk public transit systems and creates a grant program for capital and operational security improvements by public transit agencies.	H.R. 1401 and H.R. 1269 require analysis of rail communications and their proposed grant programs identify communications equipment as an eligible use of funds. Specifically, the bills include communications as subjects of research and development funding. S. 184 and S. 83 include communications as an eligible use for grants to Amtrak, freight railroads, states and localities, and rail car and hazmat suppliers. H.R. 534 and S. 763 include communications equipment as an eligible purpose for the public transit grant programs.	Rep. Bennie Thompson (D-MS), Chairman of the Committee on Homeland Security, introduced H.R. 1401 on March 8, 2007. Both House Committees approved H.R. 1401 on March 22 and the House approved the bill on March 27 by a vote of 299 to 124. The Senate received H.R. 1401 on March 28 and referred it to the Committee on Commerce, Science and Transportation. Rep. James Oberstar (D-MN), Chairman of the Committee on Transportation and Infrastructure, introduced H.R. 1269 on March 1, 2007. Sen. Daniel Inouye (D-HI), Chairman of the Senate Committee on Commerce, Science and Transportation, introduced S. 184 on January 4, 2007. The Senate Commerce Committee approved S. 184 on February 15, 2007 and the legislation was placed on the Senate Legislative Calendar on the same day. On February 17, 2007, a cloture motion was filed in an effort to bring S. 184 under consideration by the full Senate; however, the motion was withdrawn on February 27, 2007. Senator Lautenberg (D-NJ) introduced S. 294 on January 16, 2007, and the legislation was referred to the Senate Committee on Commerce, Science, and Transportation. On May 22, 2007, the legislation was reported out of Committee and placed on the Senate Legislative Calendar. S.763 was authored by Sen. Chris Dodd (D-CT), the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs, which approved the bill on March 5, 2007. Sen. John McCain (R-AZ) introduced S. 83 on January 4, 2007 and it was referred to the Senate Commerce Committee.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
S. Amdt. 2422, to the DHS Appropriations Act for FY2008, H.R. 2638	Requires a report on border areas where radio communication is unavailable or inadequate. Further requires a plan to enhance radio communication along the U.S. borders.	Legislation attempts to address the lack of radio communications for law enforcement in certain U.S. border areas.	Sen. Domenici's (R-NM) amendment was included during Senate consideration of H.R. 2638 (see discussion above).
The Security Through Regularized Immigration and a Vibrant Economy (STRIVE) Act of 2007, H.R. 1645 The Unaccompanied Alien Child Protection Act of 2007, S. 1639	Both bills are comprehensive immigration reform bills that includes a wide variety of provisions relating to border security, enforcement, and immigration reform. Attempts to improve the use of satellite communications and other technologies to ensure communication among Border Patrol agents, residents, and other security agencies. Specifically, the legislation creates a "virtual fence" with video surveillance viewable at multiple communications centers. It also provides border law enforcement with 2-way, encrypted radios with panic buttons and GPS.	Provides for use of communications to bolster border security.	Rep. Louis Gutierrez (D-IL) introduced the bill on March 22, 2007, and it was referred to the Committee on the Judiciary and the Committee on Homeland Security. Sen. Ted Kennedy (D-MA) introduced S. 1639 on June 18, 2007. The Senate procedural motion to allow a final vote on S. 1639 failed by a vote of 46 to 53 on June 28, 2007, and the legislation was returned to the Senate Legislative Calendar.
The National Hurricane Research Initiative Act of 2007, S. 931	Creates a National Hurricane Research Initiative pursuant to the January 2007 National Science Board report "Hurricane Warning: The Critical Need for National Hurricane Initiative." Supports research and a national assessment of coastal infrastructure, including communications infrastructure.	Provides for research to improve emergency communication networks, cybersecurity and damage assessments during disasters.	Sen. Mel Martinez (R-FL) introduced S. 931 on March 20, 2007, and it was referred to the Committee on Commerce, Science, and Transportation.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The DHS Authorization Act for FY2008, H.R. 1684	Establishes an Office and Assistant Secretary of Cybersecurity and Communications within DHS to identify threats to critical information infrastructure and conduct risk assessments. Authorizes research and development of more secure versions of Internet protocols and architectures.	Establishes DHS office, which will be responsible for planning and managing emergency communications in the event of a cyber attack or other disruption of critical information infrastructure.	H.R. 1684 was introduced by Rep. Bennie Thompson, Chairman of the House Homeland Security Committee, on March 26, 2007. The House approved H.R. 1684 on May 9 by a vote of 296 to 126. The Senate received H.R. 1684 on May 11 and referred it to the Committee on Homeland Security and Governmental Affairs.
The Maritime Hazardous Cargo Security Act, S. 1594	Requires procedures for transportation of especially hazardous cargo in cooperation with standards organizations and shipping industry stakeholders. Supports interoperable communications to re-establish communications when existing port security infrastructure is damaged.	Seeks to utilize communications to strengthen port security.	Sen. Frank Lautenberg (D-NJ) introduced S. 1594 on June 12, 2007, and it was referred to the Committee on Commerce, Science, and Transportation.
Military Affiliate Radio System Emergency Communication Act of 2007, H.R. 2743	Protects volunteer, high frequency Military Affiliate Radio System networks on their assigned channels or on the National Communication System Shared Resources High Frequency Radio Program (SHARES). Prohibits DHS from banning or adding technical requirements to MARS and SHARES.	Protects existing federal communications systems.	Rep. Roscoe Bartlett (R-MD) introduced H.R. 2743 on June 15, 2007, and it was referred to the Committee on Energy and Commerce.
America's Border Security Act of 2007, H.R. 3469	Authorizes use of military surveillance assets, particularly unmanned aerial vehicles at U.S. borders and increased border security infrastructure. Authorizes the construction and improvement of ports of entry at U.S. borders and requires an annual border vulnerability assessment.	Instructs DHS to use satellite and other communications technologies for secure 2-way capabilities for the U.S. Border Patrol.	Rep. Dennis Ruppersberger (D-MD) introduced H.R. 3469 on August 3, 2007 and it was referred to the House Committee on Homeland Security and the Committee on Armed Services.

EMERGENCY BROADCASTING			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The First Response Broadcasters Act of 2007, S. 1223, H.R. 2331	Authorizes an additional 25 radio stations to provide public information in emergencies. Makes first response broadcasters eligible for immediate federal assistance in a major disaster; prohibits federal confiscation from first response broadcasters; allows broadcasters access to major disaster areas. Establishes the Broadcast Disaster Preparedness Grant Program to make $10 million in grants to first response broadcasters for redundancy.	Seeks to strengthen the existing emergency alerting system.	Sen. Mary Landrieu (D-LA) introduced S. 1223 on April 25, 2007, and it was referred to the Committee on Homeland Security. Rep. Charlie Melancon (D-LA) introduced H.R. 2331 on May 16, 2007, and it was referred to the Committee on Transportation.

COMMUNICATIONS SURVEILLANCE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
Protect America Act of 2007, S. 1927	Authorizes the acquisition of foreign intelligence information concerning individuals reasonably believed to be located outside the U.S. upon a determination by the Director of National Intelligence and the Attorney General. Directs communications providers and their agents, employees, etc. to provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition. Terminates 180 days after enactment.	Authorizes communications providers to assist law enforcement in acquiring intelligence information.	Sen. Mitch McConnell (R-KY) introduced S. 1927 on August 1, 2007. The Senate approved S.1927 with an amendment on August 3, 2007 by a vote of 60 to 28, sending it to the House for consideration. The House approved the bill on August 4, 2007 by a vote of 227 to 183, sending it to the President for signing. The President signed the bill on August 5, 2007, making it Public Law No. 110-55. On August 2, 2007, Rep. Peter Hoekstra (R-MI) introduced a similar bill (H.R. 3321) in the House and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence. Subsequent action on S. 1927 makes further action on H.R. 3321 unlikely and unnecessary. On August 3, 2007, Rep. Silvestre Reyes (D-TX) introduced a conflicting bill (H.R. 3356) in the House. On a motion to suspend the current rules and pass the bill, the bill failed by a vote of 218 to 207 on August 3, 2007, when a 2/3 vote was required.

COMMUNICATIONS SURVEILLANCE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective (RESTORE) Act of 2007, H.R. 3773	Authorizes generalized, as opposed to individual, warrants for the interception of electronic communications. Authorizes interception of communications between non-US citizens outside the U.S. from within the U.S. without warrants (pursuant to court orders or emergency authority) regardless if the communications pass through the U.S. Requires notification of Congressional Judiciary and Intelligence Committees of any applications for any such court orders and use of emergency authority and audits of warrantless surveillance. States that 18 U.S.C. §§ 119, 121 and FISA (50 U.S.C. § 1801 et seq.) are the exclusive means of electronic surveillance. Sunsets on December 31, 2009.	H.R. 3773 does not provide legal immunity to electronic communication service providers for past surveillance activities that have been challenged in litigation.	House Judiciary Committee Chairman John Conyers (D-MI) introduced H.R. 3773 on October 9, 2007, and it was referred to the Judiciary Committee and the House Intelligence Committee. On October 12, 2007, both Committees reported the bill. On October 17, 2007, the full House began consideration of the bill, but it was then postponed. This legislation is intended to continue and reform the authority provided in the Protect America Act of 2007, P.L. 110-55, which terminates on February 7, 2008.
FISA Amendments Act of 2007, S. 2248 (Committee print not yet introduced, but available at Senate Intelligence Committee website)	Authorizes surveillance of persons outside the U.S. from within the U.S. for 1 year. Requires applications to FISA court for surveillance of U.S. persons outside the U.S. States that 18 U.S.C. §§ 119, 121 and FISA (50 U.S.C. § 1801 et seq.) are the exclusive means of electronic surveillance. Sunsets on December 31, 2013. Requires service providers to cooperate with authorized surveillance and provides compensation and immunity.	The Senate surveillance bill provides legal immunity to electronic communication service providers for authorized surveillance between September 11, 2001 and January 17, 2007 to prevent terrorist attacks.	The Senate Intelligence Committee approved the FISA Amendments Act of 2007 on October 18, 2007. The bill was reported on October 26 along with report No. 110-209 and placed on the Senate Legislative Calendar. The Senate Judiciary Committee held a hearing on October 31 and is scheduled to consider amendments on November 15.
The Foreign Surveillance Expedited Review Act, S. 139	Grants standing to U.S. citizens who refrain from communications due to a reasonable fear of surveillance not authorized by the Foreign Intelligence Surveillance Act (FISA) of 1978 (50 U.S.C. § 1801 et seq.). The Sixth Circuit struck down a District Court ruling challenging such surveillance based on lack of standing.	Facilitates standing of customers seeking to challenge surveillance of communications networks.	Sen. Chuck Schumer (D-NY) introduced S. 139 on January 4, 2007, and it was referred to the Senate Committee on the Judiciary.

COMMUNICATIONS SURVEILLANCE			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The National Security Letters Reform Act of 2007, H.R. 3189, S. 2088	Both bills seek to increase procedural protections for the use of "national security letters" from federal law enforcement or counterterrorism agencies that seek access to communication service provider and financial institution records. The bills provide for judicial review and a cause of action for misuse of national security letters.	National security letters are used to obtain records from communication service providers. S. 2088 expressly prohibits obtaining local or long distance phone records through with the letters.	Rep. Jerrold Nadler (D-NY) introduced H.R. 3189 on July 26, 2007 and it was referred to the House Judiciary Committee. Sen. Russ Feingold (D-WI) introduced S. 2088 on September 25, 2007 and it was referred to the Senate Judiciary Committee.
S. Amdt. 2513, to the DHS Appropriations Act for FY2008, H.R. 2638	Requires a national strategy and report on closed-circuit television (CCTV) surveillance systems.	CCTV systems are used to provide real-time video surveillance.	Sen. Lieberman's (ID-CT) amendment was included in H.R. 2638. For status information, *see* INTEROPERABILITY section above.

E-911 AND CITIZEN EMERGENCY COMMUNICATIONS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
The 911 Modernization Act, S. 93 S. Amdt. 299, to S. 4, the Improving America's Security Act of 2007	Provides immediate access to $43.5 million out of the future proceeds from the upcoming 700 MHz spectrum auction for a national IP-based emergency network. Provides priority for public safety answering points incapable of receiving 911 calls. The FY2006 budget reconciliation package (P.L. 109-171) authorized $43.5 million but this legislation provides immediate access prior to the auction. This IP-based network migration was authorized by the ENHANCE 911 Act of 2004 (P.L. 108-494).	Promotes a national IP-enabled emergency network capable of receiving and responding to all citizen-activated communications.	Sen. Ted Stevens (R-AK) introduced S. 93 on January 4, 2007. The Senate Committee on Commerce, Science, and Transportation reported the legislation on March 26, 2007. Sen. Stevens included S. 93 as S. Amdt. 299 during floor consideration of S. 4. and it was included in the H.R. 1 conference report, which was enacted into law (see status of H.R. 1/S. 4 in the 9/11 Commission Recommendations Section above).
The IP-Enabled Voice Communications and Public Safety Act of 2007, S. 428	Requires IP-enable voice service providers to provide 911 service, including enhanced 911 (E-911) service. Places IP-enabled voice service providers on regulatory parity with wireless commercial mobile radio service (CMRS) providers in terms of access to 911 equipment and protection from liability. Clarifies the right of states and localities to impose 911 fees on IP-enabled voice services for 911 and public safety purposes.	Extends 911 requirements and protections to VoIP providers.	Sen. Bill Nelson (D-FL) introduced S. 428 on January 30, 2007, and it was referred to the Committee on Commerce, Science, and Transportation. The Committee approved a substitute bill on April 25, 2007 and reported it to the full Senate on August 3, 2007 with Senate Rep. No. 110-142.

E-911 AND CITIZEN EMERGENCY COMMUNICATIONS			
Bill	**Description**	**Relevance to Communications**	**Status/Notes**
911 Modernization and Public Safety Act of 2007, H.R. 3403	Requires IP-enabled voice service providers to provide E-911 service and requires the FCC to grant these providers the same access to existing 911 network infrastructure that is provided to CMRS providers. Extends liability protection for emergencies to VoIP providers and authorizes VoIP service providers to provide customer information to public service answering points (PSAPs).	Extends 911 requirements and protections to VoIP providers.	Rep. Bart Gordon introduced H.R. 3403 on August 3, 2007. The House Energy and Commerce Committee's Subcommittee on Telecommunications held a hearing on the bill on September 19, 2007. The full Energy and Commerce Committee approved the bill on October 30. The House of Representative approved H.R. 3403 on November 14 by a vote of 406 to 1.
Alarm Customer VOIP Notification Act of 2007, H.R. 2725	Requires the FCC to write rules to inform customers about the steps they need to take to maintain the proper functioning of any alarm, security, or personal emergency response system in conjunction with VOIP service.	Addresses issues associated with the provision of emergency services by VoIP providers.	Rep. Eliot Engel (D-NY) introduced the bill on June 14, 2007, and it was referred to the House Committee on Energy and Commerce.

U.S. Department of Homeland Security

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Project SAFECOM—Generally	SAFECOM serves as an umbrella program within the Federal government—it oversees all initiatives and projects pertaining to public safety communications and interoperability. SAFECOM's goal is to allow public safety agencies and first responders to talk across disciplines and jurisdictions (Federal, state, local) via wireless radio communications systems, exchanging voice and/or data with one another on demand, in real time. SAFECOM's optimal public safety radio communications system would include: dedicated channels and priority access that is available at all times to handle unexpected emergencies; reliable one-to-many broadcast capability; highly reliable and redundant networks that are engineered to withstand natural disasters and other emergencies; the best possible coverage within a given geographic area, with a minimum of dead zones; and unique equipment designed for quick response in emergency situations.	SAFECOM is organizing a broad communications interoperability effort between first responders across the country. Discussed in the next six sections of this chart are SAFECOM's most recent projects.	The Office of Management and Budget established Project SAFECOM in October 2001. SAFECOM is managed by the DHS Science and Technology (S&T) Directorate's Office for Interoperability and Compatibility (OIC). SAFECOM serves over 50,000 local and state agencies and 100 Federal agencies. SAFECOM estimates that full interoperability could take 20 years. The 9/11 Commission recommended significant funding increases to help with communications between public safety agencies. Over the last several years, SAFECOM has released a number of reports regarding interoperability, including on public safety interoperability and VoIP, a national interoperability baseline survey, a public safety architecture framework trial, and guidelines for developing requests for proposals, among others. Several of the more detailed recent reports are discussed herein. *See* http://www.safecomprogram.gov/SAFECOM/library/default.htm. In May 2007, the OIC held an industry roundtable that brought together members of the emergency response community, the communications industry, and government officials to collaborate on key issues inhibiting establishment of interoperable communications systems for the emergency response community.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
RapidCom (SAFECOM Initiative)	Interoperability initiative for 10 high-risk urban areas (New York, Chicago, Washington, DC and the surrounding Capital Region, Los Angeles, San Francisco, Philadelphia, Houston, Jersey City, Miami, and Boston). At the incident area, RapidCom helps first responders from various disciplines and jurisdictions communicate through existing equipment that is made interoperable by a patch-panel device that interconnects various models of equipment. RapidCom's additional assistance includes: technical help in setting up the technology; development of Standard Operating Procedures (SOP) that guide all public safety officials; training in the use of the equipment; help in conducting test exercises; and assistance in establishing a regional governance structure that brings all relevant agencies together.	RapidCom is intended to enable public safety workers in these urban areas to communicate both internally and with those in other urban areas following an emergency incident.	With the initial work of RapidCom now complete, incident commanders in each of the urban areas have the ability to communicate with each other and their respective command centers within one hour of an incident. With the input of local emergency response officials, RapidCom identified and advanced five "critical success factors" essential to interoperable systems as represented in the "Interoperability Continuum" (see below). This initiative concluded with the Urban Area Summit on October 27 and 28, 2004.
Interoperability Continuum (SAFECOM Initiative)	This Interoperability Continuum is designed to help the emergency response community and local, tribal, state, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. These elements include governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications. The Continuum was established to depict the core facets of interoperability according to the stated needs and challenges of the emergency response community and will aid emergency responders and policymakers in their short- and long-term interoperability efforts.	Designed to facilitate interoperability of public safety communications.	Available to assist all principals in understanding how to achieve interoperability.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Statewide Communications Interoperability Planning (SCIP) Methodology (SAFECOM Initiative)	The SCIP Methodology outlines ten essential planning phases that states should use to create their own statewide communications interoperability plans. The phases include: 1) establishing key relationships and funding; 2) gathering information; 3) creating a project plan and roadmap; 4) identifying roles and responsibilities for the project team; 5) recruiting focus group participants and meeting preparation; 6) conducting focus group interviews; 7) analyzing data and preparing for strategic planning sessions; 8) conducting strategic planning sessions; 9) developing a statewide communications interoperability strategic plan; and 10) developing guidelines for the first 90 days of implementation.	Designed to facilitate interoperability of public safety communications.	SAFECOM and the OIC announced the SCIP Methodology on January 26, 2005. DHS designed the SCIP Methodology based on Virginia's plan to establish statewide interoperability. Available to assist in public safety communications planning.
Grant Guidance (SAFECOM Initiative)	Although SAFECOM is not a grant-making body, it has developed coordinated grant guidance to help maximize the efficiency and effectiveness with which emergency response communications-related grant dollars are allocated and spent. Specifically, in February 2007, the OIC published a set of criteria for statewide interoperability plans in the *Recommended Federal Grant Guidance for Emergency Response Communications and Interoperability Grants for Fiscal Year 2007*. These criteria were developed in support of Section I.C.5 of the 2006 Homeland Security Grant Program (HSGP), which states that "by the end of 2007, each state must develop and adopt a statewide communications interoperability plan." These criteria were developed with input from local and state officials and emergency responders. The grant guidance document has been used by the Office of Grants and Training, FEMA, and DOJ's Office of Community Oriented Policing Services (COPS).	Designed to facilitate interoperability of public safety communications.	In March 2007, OIC released a *Statewide Interoperability Planning Guidebook* that was designed to provide the designated State Interoperability Coordinators or the appropriate authority from each of the states and territories with an explanation of the statewide plan criteria, a step-by-step guide for developing an interoperability plan, and a recommended layout for the statewide plans. Detailed explanations include common questions to consider, helpful hints in completing each section, and a list of the criteria each section addresses.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability (SAFECOM Initiative)	In April 2004, SAFECOM released a Statement of Requirements (SoR), which defines the future requirements for crucial voice and data communications in day-to-day, task force, and mutual aid operations. The SoR serves as a first step toward establishing base-level communications and interoperability standards for all emergency response agencies and helps the emergency response community convey a shared vision that ultimately will help private industry better align research and development efforts with critical interoperable communication needs. The SoR is currently a two-volume set. Volume I explains the qualitative requirements and identifies the applications and services critical for public safety communications. Volume II describes the quantitative requirements and provides detailed quality of service methods of measurement for the applications and services identified in Volume I, along with network parameters to specify the minimum acceptable performance of public safety communications systems carrying these services.	Designed to facilitate interoperability of public safety communications.	In April 2006, SAFECOM released an updated version of the SoR with refinements based on input from the emergency response community. To help review and revise the SoR, SAFECOM established a working group comprised of members of the emergency response community from all disciplines with specialized expertise, knowledge, and understanding of communications technology. This working group will continue to provide on-going feedback and recommendations for future improvements to the document.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Computer-Aided Dispatch Interoperability Project (CADIP) (SAFECOM Initiative)	In August 2007, the OIC launched its Computer-Aided Dispatch (CAD) Interoperability Project, which enables computer-aided dispatch systems to exchange information across jurisdictions. The goals of this project are to study Silicon Valley, CA emergency response agencies' CAD interoperability efforts, and to identify the challenges, best practices, benefits, and costs associated with linking CAD systems across jurisdictions. In the future, the project also will work with localities that are pursuing a different approach to CAD interoperability. The project will identify approaches to linking CAD systems in order to assist local and state agencies as they migrate toward multi-jurisdictional, interoperable CAD systems. In a parallel effort, OIC is partnering with the National Capital Region to identify specific requirements for exchanging CAD information and to develop data standards enabling CAD information exchange. OIC will work with emergency responders nationwide to validate these requirements and CAD standards. This work will then be brought into standards organizations and adopted as formal standards for implementation by manufacturers.	Designed to facilitate interoperability of public safety communications.	OIC will use the results of the CADIP project to develop tools, templates, and guidance documents intended to assist agencies and jurisdictions improve CAD system interoperability with neighboring regions.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Tactical Interoperability Communication Scorecards	In January 2007, DHS released tactical interoperability communication scorecards for 75 urban/metropolitan areas that assess the maturity of tactical interoperable communications capabilities in those areas. These scorecards were developed by subject matter expert panels that reviewed documentation on current communications plans, exercises, and a self-assessment to arrive at consensus findings and recommendations for each region on how to best improve that region's communications capabilities. The scorecard evaluation specifically focuses on Governance, Standard Operating Procedures (SOP), and Usage elements of the SAFECOM Interoperability Continuum.	Designed to facilitate interoperability of public safety communications.	A more comprehensive analysis of the scorecards is being developed. DHS is continuing to align its programs and resources to best address the communications needs of first responders.
Commercial Equipment Direct Assistance Program (CEDAP)	CEDAP provides first responders with a variety of equipment, including interoperable communications equipment, and training designed to enhance state and local communities' capabilities and improve regional coordination during emergencies.	Through the provision of equipment and training, CEDAP strengthens the nation's ability to prevent, protect, respond, and recover from a disaster.	On March 27, 2007, DHS announced the award of $34.6 million in equipment and training to first responders across the nation.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
National Communications System (Generally)	The NCS assists the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack & recovery and reconstitution. The NCS has created a number of different services. NS/EP Priority Telecommunications (GETS, TSP, WPS); National Coordinating Center for Telecommunications (ACN, SHARES); Telecom ISAC; Emergency Response Training (Planning, Training, and Exercise Support); Individual Mobilization Augmentee.	Provides for emergency federal oversight for federal and non-federal communications.	After nearly 40 years with the Secretary of Defense serving as its Executive Agent, the National Communications System was transferred to the Department of Homeland Security (DHS). In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
National Emergency Communications Strategy (NCS)	In February 2006, DHS submitted to the President a document entitled the *Federal Response to Hurricane Katrina: Lessons Learned*, which outlined numerous lessons learned and identified 17 challenges facing the Federal Government, including communications and critical infrastructure protection. In response, the President directed NCS to organize an interagency group to begin development of a national emergency communications strategy. The NCS worked in partnership with a Federal interagency working group to develop a strategy and submitted the interagency interim *National Emergency Communications Strategy* to the President for further review and consideration on May 17, 2006.	Provides a framework for future U.S. Government emergency response planning efforts and informs revisions to key policy documents governing emergency communications support.	Interim strategy submitted to the President for consideration and review. In January 2007, the President's National Security and Telecommunication Advisory Committee submitted a report to the President on Emergency Communications and Interoperability. In this Report, the NSTAC recommended that several elements be incorporated into the National Emergency Communications Strategy, including yearly benchmarks for achieving defined interoperability objectives, the development of large-scale state and regional shared public safety networks and federal grants, and nationwide outreach, among other things.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
National Infrastructure Protection Plan (NIPP) and, specifically, Communications SSP (NCS)	To address the pre-existing threat of natural disasters, while factoring in the new threat of terrorism, the Department of Homeland Security (DHS) released the National Infrastructure Protection Plan (NIPP) in June 2006. The plan provides a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. The NIPP coordinates Federal departments and agencies; State, local, and tribal governments; private sector owners and operators; and international partners. To implement the NIPP, Sector-Specific Agencies (SSAs) for each of the 17 critical infrastructure and key resources (CI/KR) sectors are partnering with State, local, and tribal governments, and industry to create and implement Sector-Specific Plans (SSPs).	The Communications SSP describes a collaborative effort among the private sector, Federal Government, and State governments to protect the Nation's communications infrastructure. This collaboration will result in the assessment of risk to the communications architecture and its functions that will help prioritize protection initiatives and investments within the sector and aid the identification of critical assets against specific threats.	The Communications SSP was released in May 2007. It results from a close collaboration among the NCS, the Communications Sector Coordinating Council, and the Communications Government Coordinating Council (GCC). It provides a framework for industry and government partners to develop a coordinated protection strategy.
Route Diversity Project (RDP) (NCS)	The Route Diversity Project was established to develop a route diversity methodology and route diversity analysis capability that could analyze Federal agencies' telecommunications resiliency and redundancy. The RDP also researches and demonstrates various technical approaches that could be used to provide this service.	Aids federal agencies in improving the resiliency and redundancy of their communications networks.	The RDP continually investigates new solutions for creating a resilient network. Evaluations on Free Space Optics and satellite communications have been released. Evaluations of service offerings and white papers on various technologies are expected to be released. *See* http://www.ncs.gov/rdp/index.html under "Technology Research." Third parties may partner with the RDP to evaluate a technology or service.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Communications Resource Information Sharing (CRIS) (NCS)	The CRIS initiative establishes an information source that identifies transportable communications equipment, over-the-counter services, and fixed communications networks of the Federal government that could be used on a shared basis with other Federal organizations to support NSEP requirements. CRIS is open to all NCS member organizations (23 Federal departments and agencies) and their affiliates on a voluntary basis. Identification of telecommunications resources for use in CRIS is also on a voluntary basis, and the sharing of such resources is not to interfere with an organization's mission.	Facilitates the shared use of communications assets, services, and capabilities during an emergency.	The Executive Office of the President approved CRIS in February 1996. The NCS CRIS Working Group guides the CRIS initiative. The Chief, Operations Division (N3), NCS provides day-to-day administration of CRIS. Twenty-six Federal and industry organizations contribute resources to CRIS.
Communications Infrastructure Information Sharing and Analysis Center (ISAC) (NCS)	The ISAC's mission is to facilitate voluntary collaboration and information sharing among Government and industry in support of the protection of the nation's critical infrastructure by gathering information on vulnerabilities, threats, intrusions, and anomalies from multiple sources and performing analyses with the goal of averting or mitigating impact upon the telecommunications infrastructure.	Facilitates the sharing of information among Government and industry so that the impact of a national disaster on telecommunications infrastructure can either be averted or mitigated.	Currently, there are 41 members. The Communications ISAC is available 24/7.
Network Security Information Exchange (NSIE) (NCS)	The NSIE is an industry-Government partnership that was established to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures.	Facilitates the sharing of information and ideas among Government and industry regarding network security.	The NSIE occasionally holds ad hoc sessions to discuss security technologies and their implementation. The NSIE also provides immediate assistance to NSIE member organizations when urgent security concerns arise.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Modeling, Analysis and Technology Assessment (NCS)	NCS uses a number of modeling and analysis techniques and applications to conduct technical studies or analyses for the purpose of identifying improved approaches that may assist Federal entities in fulfilling NSEP objectives. For example, the Network Design and Analysis Capability (NDAC) analyzes different operational aspects of telecommunications networks, thereby enabling NCS to review the operation of the public switched network. NCS is also modeling and analyzing a variety of other technologies, including next generation networks, the Internet, supervisory control and data acquisition systems, and a next generation priority services experimental testbed environment. NCS has also developed a Technology Assessment Network, which enables the evaluation of cutting edge technology without jeopardizing existing development or production of systems and a Technology Assessment and Data Analysis Cell, which will provide NCS with a fully accredited facility capable of evaluating contract deliverables and products, hosting applications and databases, providing component-level simulation, participating in community research projects, and training.	These techniques detect and help mitigate damage caused by disasters and assists in reconstitution of telecommunications networks. They also assist in the development of future networks.	These activities remain ongoing and the techniques are continually refined and expanded through software updates and application development.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Advanced Technology Group (ATG) (NCS)	The ATG investigates new and emerging technologies with the objective of making them available to Government during national emergencies or crises. Specifically, the ATG has performed studies on Telecommunications Electromagnetic Disruptive Effects and has published a number of technical reports concerning vulnerability issues associated with the telecommunications infrastructure and emerging wireless and wireline communications technologies, such as satellite communications, the Alerting and Communications Network, and the Global Positioning System, and their impact on NSEP telecommunications services.	Furthers the use of new and evolving technologies by government agencies during emergencies.	The ATG's studies remain ongoing. Among other things, the ATG is introducing concepts to solve credentialing using satellite technologies, in addition to investigating priority satellite communications for NSEP.
Continuity Communications Working Group (NCS)	The Continuity Communications Working Group addresses stove-piped systems and the lack of interoperability between Federal Executive Branch departments and agencies in their continuity communications infrastructure.	Facilitates the continuity of federal government communications.	In 2006, the Continuity Communications Working Group was reconstituted under the NCS' Committee of Principals. The Working Group's efforts remain ongoing.
National Coordinating Center for Telecommunications (NCC) (NCS)	The NCC is the primary mechanism within the NCS for fulfilling the emergency response role. The NCC's mission is to assist in the initiation, coordination, restoration and reconstitution of NSEP telecommunications service or facilities under all conditions, crises, and emergencies.	Coordinates the restoration and provisioning of NSEP telecommunication services and facilities during natural disasters and armed conflicts.	The NCC's work is ongoing.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Alerting and Coordination Network (ACN) (NCS)	The ACN was designed to provide a survivable emergency communications network connecting critical telecommunications service providers' network operations and/or emergency operation centers with key federal entities.	Provides a stable voice communications network for restoration coordination, priority transmissions, and incident reporting when the public switched network is inoperable.	The NCS is in the process of implementing new ACN capabilities and technical architecture.
National Response Framework	The National Response Plan, last updated May 25, 2006, establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines and integrates them into a unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. On September 10, 2007, DHS released a draft National Response Framework, the successor to the National Response Plan. The Framework, which focuses on response and short-term recovery, articulates the doctrine, principles and architecture by which our nation prepares for and responds to all-hazard disasters across all levels of government and all sectors of communities. The Framework is responsive to repeated federal, state and local requests for a streamlined document that is shorter, less bureaucratic and more user-friendly.	Addresses the role of communications networks and personnel during emergencies and the necessity for accurate and timely communications among government users and with the public.	Comments on National Response Framework were due October 10, 2007. The National Response Plan remains in effect during this comment period.

NETWORK SECURITY AND RELIABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
National Strategy to Secure Cyberspace	The National Strategy to Secure Cyberspace outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity.	This strategy is part of an overall effort to protect the Nation by engaging and empowering Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.	The National Strategy to Secure Cyberspace was released in 2003.
Cyber Security Awareness Month	The National Cyber Security Alliance, a consortium of government agencies and private industry sponsors, has declared October as National Cyber Security Awareness Month. National Cyber Security Awareness Month is a national campaign designed to increase the public's awareness of cyber security and crimes issues, so that users can take precautions to avoid these threats on the Internet.	Maintaining cyber security is essential to protect the integrity and functioning of the nation's communications infrastructure.	National Cyber Security Awareness Month began in October 2004.

PRIORITY SERVICE			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Priority Services Working Group (PSWG) (NCS)	The PSWG was established to undertake (1) an evaluation of the NCS' GETS, TSP, and WPS programs; (2) an examination of priority service outreach efforts; (3) an assessment of cost issues; and (4) an analysis of the potential impact of future technologies on priority services programs.	Provides recommendations on how priority service programs can be improved.	The PSWG's review is ongoing. In 2006, the PSWG completed a report on the Telecommunications Service Priority Program.
Telecommunications Service Priority (TSP) (NCS)	The TSP program provides the framework for the priority restoration and provisioning of any qualified national security and emergency preparedness (NSEP) telecommunications services. NSEP services are those services used to maintain a state of readiness or manage any emergency (local, national, or international) that harms the population, damages property, or threatens the NSEP posture of the U.S. A restoration priority is assigned to new or existing telecommunications services to ensure restoration before non-TSP services. Priority restoration should be assigned to a new service when interruptions may have a serious, adverse effect on the supported NSEP function. A provisioning priority facilitates priority installation of new telecommunications services. Provisioning on a priority basis becomes necessary when a service user has an urgent requirement for a new NSEP service that must be installed quickly.	Facilitates emergency provisioning and repair of certain communications services.	In 1988, the FCC issued a Report and Order (FCC 88-341) establishing the TSP Program. Currently there are over 109,000 total active TSP assignments in support of NSEP communications. During FY 2006, over 32,000 TSP codes were added, changed or revoked. Additionally, the TSP user base increased by approximately 128 new organizations, bringing the total number of organizations with active TSP codes to over 680. In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to explore enhancements to the TSP program to accommodate expanded requests from national NSEP users of wireless telecommunications services at critical sites.

PRIORITY SERVICE			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Government Emergency Telecommunications Service (GETS) (NCS)	Provides NSEP users with emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) when their normal telecommunications means are unavailable or congested during an emergency. GETS calls receive priority treatment through enhanced routing, controls such as trunk queuing, trunk sub-grouping, and trunk reservation, and through exemption from restrictive network management controls used to reduce network congestion. GETS is accessed through a universal access number and Personal Identification Number (PIN) card. Once the caller is authenticated, his or her call receives priority treatment.	Facilitates access to wireline communications services by certain entities in an emergency.	The President directed the Office of the Manager, NCS (OMNCS) to develop GETS. On 9/11, 18,000 GETS calls were made (10,000 in NY and DC), and the call completion rate exceeded 95%. During the 2001 Nisqually Earthquake near Seattle, there were 400 successful GETS calls. As of September 30, 2006, there were 140,743 active GETS cards—an increase of 30,283 cards since September 2005.
Wireless Priority Service (WPS) (NCS)	During emergencies, cellular networks can experience congestion due to increased call volumes and/or damage to network facilities. Wireless Priority Service was developed to provide priority for emergency calls made from cellular telephones. Wireless Priority Service is implemented as software enhancements to cellular networks, and is being deployed by cellular service providers in their coverage areas throughout the United States.	Facilitates access to wireless communications services by certain entities in an emergency.	As of September 30, 2006, there were 38,668 authorized WPS users—a 51 percent increase since September of 2005. In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to expand and enhance use of the WPS program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi-carrier WPS end-to-end solutions that facilitate the rapid restoration of essential wireless network elements.

EMERGENCY ALERTING			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Digital Emergency Alert System (DEAS)	The Digital Emergency Alert System is testing how the digital capabilities of the nation's public radio and television stations and other networks—combined with the voluntary participation of cell phone service providers; public and commercial radio and television broadcasters; satellite radio, cable, and Internet providers; and equipment manufacturers—can be used to provide alert and warning information to the public and to disaster support personnel.	Utilizes existing communications infrastructure to expand the alerting system so that everyone, regardless of location or time of day, will receive emergency information.	The national DEAS pilot will run for 1 year beginning in January 2007, with all public broadcasting stations (over 300 nationwide) to be DEAS-enabled by December 2007 Overall, the new warning system is expected to cost $4.5 million to test and deploy nationally, and $1 million annually to maintain.
Shared Resources High Frequency Radio Program (SHARES) (NCS)	SHARES brings together existing HF radio resources of federal, state, and industry organizations to provide a single, interagency emergency message handling system for Federal departments and agencies. Certain conditions must exist to use SHARES, including: the information must support NSEP requirements; the information must be communicated to a Federal entity and be of critical importance to the Federal government, the entity's mission, and/or involve the preservation of life and property; the primary means of communications must be inoperative or unavailable for use; and the processing of SHARES message traffic must not interfere with the primary mission requirements of the SHARES participants. To access SHARES, a user contacts the nearest SHARES station listed in the SHARES Directory and requests assistance in processing a SHARES message. SHARES is available on a 24/7 basis.	More than 250 designated frequencies have been authorized for use in SHARES.	SHARES stations are located in every state and at 20 overseas locations. 194 emergency planning and response personnel participate. A SHARES Bulletin is published periodically to keep members updated on program activities. The SHARES HF Interagency Working Group, consisting of 154 members representing 110 organizations, conducts three nationwide readiness exercises each calendar year, which provides personnel training on operating procedures and various message formats, expands SHARES awareness within the Federal emergency response community and assesses the interoperability of new HF technologies.

OTHER			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
People Access Security Service (PASS) System. DHS Proposes to Expand the Use of Vicinity RFID in Implementing Western Hemisphere Travel Initiative	The Department of Homeland Security (DHS), in conjunction with the Department of State's proposed rulemaking on the new PASSport card, announced in October 2006 that it proposes to expand the use of vicinity radio frequency identification (RFID) technology at U.S. ports of entry. The vicinity RFID technology, to be compatible with the PASSport card, would allow a travel document to be read from several feet away as a vehicle approaches inspection. The proposed PASSport card would serve as an alternative to a traditional passport book for use by U.S. citizens who cross the land borders and travel on cruises to Canada, Mexico and the Caribbean. It would provide evidence of identity and citizenship, be convenient to carry, and cost less than the traditional passport book.	PASS utilizes communications technology to address border security issues.	The proposed regulations of the PASSport card were published by the Department of State in the Federal Register on October 17, 2006. The comment cycle on this Proposed Rule has closed.

U.S. Department of Justice

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Integrated Wireless Network (IWN)	IWN is a joint effort by the DOJ, DHS, and the Treasury to provide a consolidated nationwide federal wireless communications service that replaces stand alone component systems and supports first responders and law enforcement with integrated communications services (voice, data, and multimedia). IWN is governed by the IWN Executive Board, which is comprised of the CIOs from DOJ, DHS, and Treasury. The government estimates that IWN should take between 5-10 years to complete. The estimated funding for IWN is $2.5 billion (however, the ceiling is $10 billion). The government estimates that IWN will serve over 80,000 law enforcement users and will operate through 2,500 sites.	IWN will implement solutions to provide federal agency interoperability with appropriate links to state, local, and tribal public safety and homeland security entities.	General Dynamics has been selected as the IWN integrator. The contract with General Dynamics is also available for use by the other IWN partners.
High Risk Metropolitan Assistance Project: the 25 Cities Project	This project addresses the following request from the House/Senate CJS Appropriations Subcommittee staff to the DOJ Wireless Management Office (WMO): (1) provide federal law enforcement/ homeland security agencies with basic inter-systems communication for emergency situations; (2) provide an ability to connect with key local authorities (*i.e.*, fire, police, emergency medical services [EMS]); and (3) address the top 25 metropolitan areas that are likely targets for attack. The WMO has applied a five-phased approach and has worked in tandem with federal, state and local representatives in each city to develop mutually agreeable and unique interoperability solutions tailored to that city/region; where applicable, DOJ has leveraged existing communications infrastructure and ongoing local area interoperability initiatives	Project is designed to enhance the effectiveness and interoperability of law enforcement communications.	In May 2005, the DOJ reported on its efforts to date. This Project remains ongoing.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Community Oriented Policing Service (COPS) Interoperable Communications Technology Program	The COPS Interoperable Communications Technology Program provides funding to help communities develop effective interoperable communications systems for public safety and emergency services providers. Interoperable Communications Technology grants fund projects that explore uses of equipment and technologies to increase interoperability among the law enforcement, fire service, and emergency medical service communities. These projects are the result of thorough planning and demonstrate how new technologies and operating methods can help communities achieve interoperability.	Aids in the research and development of technology for communications interoperability.	In 2006, the COPS Office awarded $8.8 million to three law enforcement agencies to address the growing need for interoperable communications technology. To date, COPS has awarded more than $250 million to 65 communities to improve their interoperable communications systems.
CommTech Program	CommTech is a comprehensive interoperability project targeted at state and local law enforcement agencies. CommTech is developing open architecture standards for voice, data, image, and video communications systems. These standards will help users exchange information among fixed facilities, mobile platforms, and personal devices. CommTech also researches, develops, tests and evaluates technology solutions that facilitate interoperability in a test bed environment. Areas of interest include VoIP; standards-based radios/systems; cognitive radio; software-defined radio; wireless broadband data communications; antenna research; in-building coverage; multi-band radio; and network coverage extension for rural environments.	CommTech facilitates communications interoperability among state and local law enforcement agencies.	Operated through the DOJ's National Institute of Justice (NIJ). The interoperability standards that CommTech ultimately develops will be incorporated into a Strategic Plan that law enforcement agencies can use to achieve interoperability. NIJ funds communications technology research and development through directed solicitations.

U.S. Department of Commerce

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Spectrum Management for the 21st Century: Plan to Implement Recommendations of the President's Spectrum Policy Initiative	In June 2003, President George W. Bush established the Spectrum Policy Initiative to further develop and implement a U.S. spectrum policy for the 21st century that meets the Nation's needs and spurs economic growth. After establishing a task force to consider these issues and seeking comment from the private sector, the Department submitted two reports to the President that reflect the views obtained in June 2004. These reports contained far-reaching recommendations on a wide range of issues. In November, 2004, the President directed the Department to submit a plan to implement the recommendations. In March 2006, NTIA released a report outlining seven projects that would implement the recommendations of the two reports: (1) Improve Stakeholder Participation and Maintain High Qualifications of Spectrum Managers; (2) Reduce International Barriers to U.S. Innovations in Technologies and Services; (3) Modernize Federal Spectrum Management Processes with Advanced Information Technology; (4) Satisfy Public Safety Communications Needs and Ensure Interoperability; (5) Enhance Spectrum Engineering and Analytical Tools; (6) Promote Efficient and Effective Use of Spectrum; and (7) Improve Planning and Promote Use of Market-based Economic Mechanisms in Spectrum Management.	To further develop and implement a U.S. spectrum policy for the 21st century that meets the Nation's needs and spurs economic growth, President George W. Bush established the Spectrum Policy Initiative in June 2003.	NTIA's efforts to complete these projects remains underway. Among other things, NTIA has already established a Spectrum Management Advisory Committee, which is considering a wide variety of issues including how to implement a spectrum sharing test bed.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
A Public Safety Sharing Demonstration	On June 8, 2007, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) released a report, "A Public Safety Sharing Demonstration," analyzing the District of Columbia's Wireless Accelerated Responder Network (WARN). The WARN pilot is a city-wide broadband wireless public safety network. The system uses commercial broadband technology for remote surveillance, chemical and biological detection and several other emergency related services. The report encourages the federal, state and local public safety community to consider utilizing commercial technologies in satisfying broadband interoperable communications among first responders. The report also recommends that agencies consider commercial broadband services, when feasible.	Intended to improve management of the nation's airwaves, by addressing planning, usage and sharing of spectrum, and the feasibility of using commercial services to meet the increasingly complex wireless broadband needs of public safety.	The report is available on NTIA's website at http://www.ntia.doc.gov/reports/NTIAWARNReport.pdf. The report's recommendations may be used in the further development and implementation of public safety communications and spectrum policies.

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Public Safety Interoperable Communications Grant Program	NTIA and DHS signed a Memorandum of Understanding on Friday, February 16, 2007, to implement the Public Safety Interoperable Communications Grant Program to help state, local and federal first responders better communicate during a natural or man-made disaster.	The grant program, which covers public safety agencies in all 50 states, the District of Columbia, Puerto Rico and four U.S. territories, will assist public safety agencies in the acquisition, deployment, or training for the use of interoperable communications systems that can utilize reallocated public safety spectrum in the 700 MHz band for radio communication.	On July 18, 2007, U.S. Commerce Secretary Carlos M. Gutierrez and U.S. Homeland Security (DHS) Secretary Michael Chertoff announced the availability of $968 million in Public Safety Interoperable Communications Grants to help state and local first responders improve public safety communications and coordination during a natural or man-made disaster for all 50 states, the District of Columbia, and the U.S. territories. Public safety organizations interested in PSIC funding will be able to seek funding through their State Administrative Agency. The deadline for submission of each State and Territory's Investment Justification is December 3, 2007.

U.S. Department of Agriculture

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
Rural Information Center (RIC)	The Rural Information Center provides information and referral services to local, tribal, state, and federal government officials; as well as community organizations, rural electric and telephone cooperatives, libraries, businesses, and citizens working to maintain the vitality of America's rural areas. RIC also provides resources for communications interoperability and emergency preparedness.	RIC provides resources to local officials to improve emergency communications in rural areas.	RIC has released publications such as Rural Homeland Security Resources for Local Officials and Rural Fire Department Resources for Local Officials, which provide lists of planning and training resources for local officials as well as information on funding and program assistance.

U.S. Department of Health and Human Services

INTEROPERABILITY			
Initiative	**Description**	**Relevance to Communications**	**Status/Notes**
The Emergency Preparedness Resource Inventory (EPRI)	EPRI is a web-based tool allowing local or regional planners to assemble customized inventories of critical resources that would be useful in responding to a bioterrorist attack, including health care and emergency resources. The tool uses the Internet so communities can assess their regional supply of critical resources, prepare for incident response, estimate gaps, support future resource investment decisions, and help first responders figure out where emergency equipment and medicines are located, how much is available, and whom to contact to obtain those resources.	This tool utilizes the Internet to disseminate emergency information to local and regional governments.	Released by HHS' Agency for Healthcare Research and Quality in May 2005.
New Emergency Information Center Model	This operations model for emergency call centers is designed to help public health agencies and other first responders prepare to provide accurate, timely information during a health emergency. The model is also designed to help public health departments, state and local officials and others gear up quickly to answer calls from the public and health care providers if an emergency arises.	The model offers guidance to organizations on the requirements, specifications and resources needed to develop a public health emergency contact center that is highly integrated with public health agencies and that can reduce the likelihood of hospitals and health systems being overwhelmed with calls and requests for information.	Released by HHS' Agency for Healthcare Research and Quality in March 2005. The model is available for download at the HHS Agency for Healthcare Research and Quality website. A goal of the model is to develop the capacity to handle 1,000 calls per hour from health care providers or members of the public in addition to delivering regular services.